北京金融科技产业联盟
BEIJING FINTECH INDUSTRY ALLIANCE

金融网络安全运营数智化建设研究与实践

北京金融科技产业联盟

2026 年 4 月

版权声明

本报告版权属于北京金融科技产业联盟，并受法律保护。转载、编摘或利用其他方式使用本白皮书文字或观点的，应注明来源。违反上述声明者，将被追究相关法律责任。

编制委员会

编委会成员

黄程林　巫建刚　王　磊　赵海权　张　勇　张立文

编写组成员（排序不分先后，按姓氏拼音排序）

陈代乐　陈　明　陈宇磊　董润汉　段　超　龚兴超　胡　飞

胡宏伟　李万宝　李尚泽　刘凯宇　茅雨绮　苏　涵　孙德福

孙　钢　特荣夫　王　畅　王海星　夏海蛟　徐春运　张信保

张　帆　张　牧　张文博　张　毅　赵殷豪　周　涛

编审

黄本涛　刘昌娟

牵头单位

中国邮政储蓄银行股份有限公司

参编单位

国家开发银行

中国银联股份有限公司

兴业银行股份有限公司

浙商银行股份有限公司

北银金融科技有限责任公司

北京银联金卡科技有限公司

深圳市腾讯计算机系统有限公司

北京天融信网络安全技术有限公司

摘 要

随着数字化转型的深入推进，网络安全已成为关乎金融稳定与客户信任的核心保障。面对日益频繁的网络攻击、数据泄露和高级持续性威胁，传统依赖人工的被动防御模式已难以应对，银行业亟需推动网络安全运营向数智化转型，通过融合大数据、人工智能等前沿技术，构建智能、主动、自适应的安全防护体系，为金融业务创新与发展筑牢战略安全底座。

本报告围绕金融网络安全运营数智化建设展开系统研究，阐述了在日益复杂的网络威胁背景下，传统安全运营模式存在的效率低下、响应滞后等问题，指出引入大数据、人工智能、大模型等技术的必要性。从核心内涵、关键技术、体系架构、流程重构等方面深入探讨，提出以数据中台、AI 模型、SOAR 平台等为核心的技术架构，并设计了“事前-事中-事后”全周期运营流程。最后，结合银行业实践，指出未来网络安全运营将向“智能泛在、生态协防、人机协同”方向发展，形成新的智慧网络安全运营体系。

关键词：网络安全运营 数智化 大模型 人工智能 智能分析 自动化响应

目 录

一、总体概述.....1

（一）背景意义.....1

（二）发展现状.....1

（三）研究内容.....4

二、核心内涵与关键技术.....4

（一）基本概念.....4

（二）关键支撑技术.....7

三、体系设计与实践路径.....9

（一）网络安全数智化运营技术架构.....9

（二）运营流程的数智化重构.....12

（三）关键成功要素与持续运营机制.....13

四、实践案例.....15

（一）邮储银行构建网络安全运营数字化底座.....15

（二）北银金科聚焦高危场景践行“AI+SOAR”.....22

（三）兴业银行借助大模型智能体重构安全运营.....25

（四）浙商银行构建“一基础五平台”数智化防护体系.....28

五、未来展望.....31

（一）AI 重塑安全运营内核.....31

（二）构建开放共生安全生态.....31

（三）重塑安全团队组织形态.....32

一、总体概述

（一）背景意义

当前，互联网技术飞速发展，网络空间已成为现代社会不可或缺的一部分，极大地促进了信息的流通与共享，同时也带来了前所未有的安全挑战，网络攻击频发、数据泄露风险增加、高级持续性威胁（APT）等安全事件层出不穷，严重威胁着国家安全、社会稳定以及个人隐私。

面对上述挑战，传统的网络安全运营模式往往依赖于人工分析和响应，存在效率低、响应慢、覆盖面窄等问题，难以有效应对日益复杂的网络安全威胁。网络安全运营亟需通过运用大数据、人工智能、机器学习等先进技术，向数智化转型，实现对网络安全威胁的实时监测、智能分析和快速响应，显著提升网络安全运营的效率和效果。探索网络安全运营数智化建设的路径及实践，促进银行业提升网络安全防护能力、保障网络空间安全。

（二）发展现状

利用大模型为网络安全赋能已成为安全界的热点研究方向。据 Gartner 统计，生成式网络安全 AI，可以提高效率并缩短对网络安全风险和威胁的响应时间，实现自动化值守，自主基于高级指引运行，而不需要频繁提示对话。目前国内主流安全厂商陆续发布安全大模型相关产品，安全大模型已经成为网络安全的新赛道。

利用大模型，为网络安全赋能的场景也越来越丰富，涵盖了

安全运营分析的各个阶段，以下是目前比较主流的典型场景：

1.搜索与威胁狩猎：利用大模型更强的语意识别、理解和关联能力，使用自然语言进行搜索，降低技能门槛，提高结果的准确性和全面性，降低运维人员搜索与威胁狩猎门槛；

2.安全信息摘要：自动生成摘要和关联性视图，扩展集成知识库，协助问题理解和处置；

3.攻击路径摘要：自动对复杂操作、漏洞利用和攻击行为进行建模，模拟攻击路径，并创建易于理解的摘要，协助风险评估和处置，如攻击定性、风险研判、攻击面和影响面管理、补救和缓解措施生成等。

4.改善情报运营：能更有效地实现论坛、暗网、深网的踪迹识别，以及信息传递混淆，同时善于进行跨数据源的信息关联，并生成更容易阅读的摘要或报告，提高威胁检测效率，降低分析者门槛。

5.数据标签和摘要：将手工标注变为自动化标注。大模型非常善于理解数据内容，结合无监督和有监督的机器学习，辅助数据管理人员实现自动化的标注，提高分类分级或其他安全策略关联的效率。

6.恶意脚本分析：经过大量恶意脚本进行预训练的模型，能够自动生成代码分析摘要和报告，发现容易被忽略的隐患，更准确甄别正常脚本，从而辅助分析人员提升分析效率，减少对高阶专家的依赖，提供稳定的质量输出，减少漏报和误报。

7.逆向代码分析：经过大量代码和反编译进行预训练的模型，能够自动进行逆向补全和函数名称与功能摘要的生成，逆向工程师无需破译每一行代码，便能快速、高层次地理解代码功能。

8.Web 安全分析：经过大量 Web 攻击流量进行预训练的模型，能够有效提升 Web 潜在风险的识别并给出修复意见。

有研究表明，目前大模型技术赋能网络安全运营已深入到运营工作的各个环节，以 IPDRR 模型为例，相关赋能活动成熟度如图 1。



图 1 大模型技术赋能网络安全运营成熟度

短期来看，大模型将显著提升现有安全技术的性能和智能化水平。得益于大模型在数据理解、意图识别、任务编排等方面的能力，在安全问答、安全运营、数据分类分级、违规处理个人信息检测、音视图文内容安全检测等关键网络安全场景中，大模型能够在大幅减少人工参与的同时，有效提升安全事件处理的效率

和准确性。

长期来看，大模型有潜力成为安全防护的核心，从而改变安全的工作模式。当前，大模型主要扮演安全从业人员的辅助工具，用于提高他们的工作效率和效能。未来，随着大模型在自主研判和决策能力方面的提升，预计将进化为安全从业人员的合作伙伴，共同应对安全风险的识别、防御、检测、响应和恢复等一系列复杂工作。

（三）研究内容

本课题旨在全面系统研究网络安全运营数智化建设的相关问题。首先，分析网络安全运营数智化的背景、意义及发展现状；其次，从理论基础、关键技术等方面入手，深入探讨网络安全运营数智化建设的核心要素；再次，通过银行业典型机构的实践经验，体现数智化建设在提升网络安全运营效率和效果方面的实际效果；最后，针对当前面临的挑战提出应对策略，并对未来发展趋势进行展望。

二、核心内涵与关键技术

（一）基本概念

1.核心定义与特征

1）网络安全运营

本课题所研究的网络安全运营，是指组织在生产运行环节，为持续监控、检测、分析、调查、响应和防御网络安全威胁而建立的一套人员、流程和技术的综合体系。其核心目标是主动保护

组织的关键信息资产、系统、网络和数据免受损害，并将安全事件的影响降到最低。

2）数字化、智能化、数智化转型

所谓数字化转型，是指深化应用新一代信息技术，激发数据要素创新驱动潜能，建设提升数字时代生存和发展的新型能力，加速业务优化、创新与重构，创造、传递并获取新价值，实现转型升级和创新发展的过程。推进数字化转型，通常坚持以价值效益为导向、以新型能力为主线、以数据要素为驱动、以业务变革为核心。[①]

所谓智能化转型，是指在数字化转型基础上，引入人工智能等智能技术，实现从“数据驱动”向“智能驱动”的转变，核心目标是提升运营、战略及社会价值。数智化转型作为数字化转型的高阶表现，使业务活动更加智能地感知、认知、决策、行动，从而极大地提升业务效率，成为新时代支撑企业业务运营的重要生产力。[②]

所谓数智化转型，在“十五五”规划建议的官方解读中，是指强调在数字化的基础上，引入智能化技术，如自主学习、决策优化、预测分析等，从而提高生产效率、优化资源配置、提升管理水平、强化创新能力。[③]

3）网络安全运营数智化

本课题所研究的网络安全运营数智化，旨在讨论在网络安全

[①] GB/T23011—2022，3.3
[②] 中国信息通信研究院（CAICT）《企业智能化转型发展研究报告（2022）》
[③] 《人民日报》（2025 年 11 月 26 日）

运营领域，如何实现传统网络安全运营模式的数智化转型。即利用 AI、大模型、数据融合等技术，实现从数据感知、智能分析到闭环处置的全流程自动化运营系统，强调“数据驱动”“智能闭环”和“自适应响应”。打造以“AI+安全运营”为核心的安全运营中心，利用数据分析和人工智能技术，及时发现外部恶意攻击威胁和资产风险，建立动态及主动的安全监测和感知机制，提高对内外部信息安全事件的预警及响应处置速度。

2.演进动因与目标价值

网络安全运营框架是指导网络安全工作的重要基础。传统网络安全运营框架往往侧重于被动防御和事后响应，难以有效应对日益复杂的网络威胁。而数智化网络安全运营框架则强调主动防御、智能分析和持续优化，以实现对网络安全的全面掌控。

传统网络安全运营框架通常包括安全策略制定、安全风险评估、安全事件监测、安全事件响应以及安全审计等环节。这些环节虽然构成了网络安全运营的基本流程，但在面对快速变化的网络威胁时，往往显得力不从心。

数智化网络安全运营框架在传统框架的基础上进行了全面升级。引入大数据分析、人工智能、机器学习等先进技术，构建以数据为核心、以智能为驱动的全新运营模式。数智化框架强调数据的实时采集与智能分析，通过自动化和智能化的手段实现安全事件的快速响应和精准处置。同时，还注重安全运营的持续优化和闭环管理，确保网络安全防护能力的不断提升。数智化网络

安全运营使网络安全运营工作从“规则驱动”走向“经验迁移+推理决策”，从“被动响应”走向“主动预测”，推动运营向高效、低依赖、强联动演化。

（二）关键支撑技术

1.人工智能与机器学习技术

人工智能和机器学习技术使系统能够自主学习和适应变化。在网络安全领域，这些技术被用于构建智能风险评估模型、自动化威胁识别系统以及基于 AI 的决策支持系统。通过不断学习和优化算法模型，AI 系统能够更准确地预测和应对网络威胁。

通过搭建安全场景知识库，实现多智能体协作架构（如采集Agent、分析 Agent、执行 Agent),基于多模型动态适配(如 Qwen、Deepseek），对多源告警数据智能分析，包括异常行为检测、误报识别、攻击路径推理等。该模式不仅增强了数据分析的全面性和深度，而且为不同场景下的告警分析提供了灵活高效的解决方案，满足需求的多样性。

通过提示词工程优化大模型推理效果，可实现自动化分类和处置建议生成。融合专家经验的研判流程建模，通过逆向分析运营人员的研判逻辑，将告警分类、上下文关联、误报验证等核心步骤抽象为自动化流程。从而构建从数据采集到决策输出的端到端自动化分析闭环，替代传统的人工研判流程，提升分析效率和准确性，减少专家经验依赖。

2.大数据分析技术

大数据分析技术能够处理海量、复杂的数据集，提取有价值的信息和模式。在网络安全运营中，大数据分析技术被广泛应用于安全日志分析、流量异常检测、用户行为分析等领域，帮助安全团队及时发现潜在的安全威胁。

网络安全日志处理方面，通过大数据技术对原始日志统一采集、清洗、富化、映射、存储等操作，实现不同安全日志类型格式标准化和日志存储统一化，解决各类安全设备和系统的数据孤岛问题。

安全态势感知方面，以大数据分析技术为支撑，通过主动关联分析海量告警日志，发现潜在威胁，建立安全数据汇聚、检测预警、分析研判、协同防御、安全可视于一体的安全运营中心，从而准确地获知网络安全态势和快速响应安全事件，推进安全防护体系从被动式向主动式转变，提升主动应对安全威胁的检测能力和对内、外部信息安全事件预警及响应处置速度。

3.自动化与编排技术

应用安全编排自动化与响应（SOAR）技术，通过灵活的剧本编排，对安全工具、专家经验及运维操作进行规划、整合、合作和协调，从而将人、过程和技术结合起来，对跨多个技术范式的运营流程及安全事件进行自动化响应，解放安全运营人力，大幅提升安全运营工作效能。一是将专家经验转化为 SOP。将安全运营过程中的一系列分析、判断、决策、优化任务封装为标准的自

动化动作，通过动作间的有机组合固化专家的安全运营经验，形成剧本以完成不同场景下的安全运营任务。二是将安全设备能力原子化。通过 API、命令行、本地脚本等手段，接入全安全设备，并依据企业安全能力框架将各设备解构并重整为标准原子化能力，使剧本能够根据安全运营需求及目标对安全设备进行动态敏捷调度。

4.云原生与弹性架构

利用云原生高可用、快速恢复和弹性特性，对安全运营服务应用进行多 pod 部署，实现应用高可用，根据服务使用资源情况，动态扩展，充分利用资源；通过建立有效的健康探测策略，可快速识别应用健康情况，及时恢复，保证安全运营应用的可靠性，为安全运营提供技术稳定性保障。

三、体系设计与实践路径

（一）网络安全数智化运营技术架构

1.设计原则

为确保银行业网络安全数智化运营架构的先进性、适用性与可持续性，其设计应遵循以下核心原则：

1）数据驱动决策原则：所有安全决策、分析和行动都应基于全面、准确、及时的安全数据。构建统一的安全数据中台，汇聚、治理、标准化所有内外部安全数据（日志、流量、资产、漏洞、威胁情报等）。

2）智能自动化原则：最大程度地利用人工智能、机器学习、

自动化编排与响应技术，提升运营效率和精准度。部署 AI 模型用于异常检测、UEBA、恶意文件分析等；通过 SOAR 平台将标准化的响应流程剧本化、自动化，实现“检测-响应-恢复”闭环的分钟级甚至秒级完成。

3）平台化与开放性原则：构建一个弹性、可扩展、松耦合的技术平台，避免新的“烟囱”系统。采用微服务、API 驱动的架构，便于新安全能力和工具的快速集成与部署。平台应具备开放接口，支持与外部威胁情报平台、监管报送系统、ITSM 系统等无缝对接。

4）持续演进与度量导向原则：安全运营是一个持续改进的过程，需要通过量化指标来衡量其有效性并指导优化方向。可以建立关键安全运营指标（如 MTTD 平均检测时间、MTTR 平均响应时间、告警准确率、自动化处置率等），通过数据看板持续监控，驱动架构、流程和技术的螺旋式上升。

2.技术架构设计

基于上述原则，本课题提出一种网络安全数智化运营技术架构，详细架构如图 2。

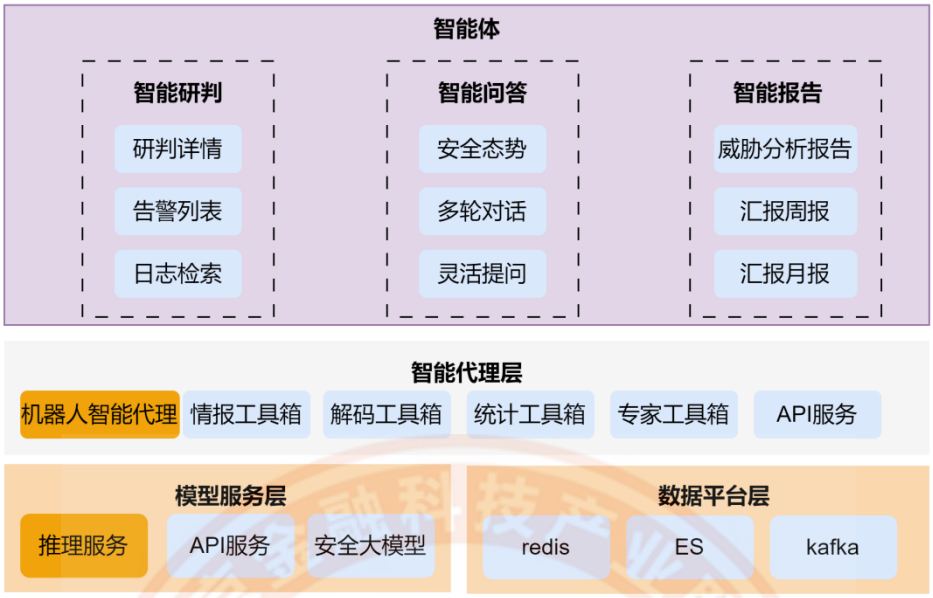


图 2 网络安全数智化运营技术架构设计图

该架构主要包括模型服务层、数据平台层、智能代理层、智能体等主要构成部分。

1）模型服务层：提供模型推理计算所需的运行时环境，以及针对不同 GPU 架构进行适配与优化以保障模型运行在最佳效率。推理服务根据安全大模型处理告警分析等；安全大模型是针对安全分析训练的模型；API 服务为外部调用提供支持。

2）数据平台层：数据平台层负责存储模型各功能模块及推理计算所需的各类数据。包括关系型数据库、缓存数据库、文档型数据库；负责提供基础大数据分析、存储能力。提供消息队列中间件以及各种分布式计算存储组件，从而支持整体系统的大量数据存储以及对内对外的大量数据处理。

3)智能代理层：主要依靠智能代理根据模型开展不同任务，也能根据任务各步骤所需以工具箱形式提供支持。封装底层大模

型能力，并给业务层服务提供调用接口，支撑各个业务的智能场景。在智能代理层预置了很多工具，以加强安全机器人的能力。例如：情报工具箱，赋能机器人获取最新威胁情报，辅助智能研判；解码工具箱，智能识别和解码告警中编码后的数据，辅助运营人员更快捷地分析异常告警；统计工具箱，智能统计系统中各类指标数据，赋值生成智能报告。

4）智能体：对安全运营工作流程和操作习惯进行优化后的交互界面，对智能研判、智能问答及智能报告提供交互操作，也能够提供多模态交互形式。

（二）运营流程的数智化重构

网络安全运营数智化建设，除了技术架构的建立，还需建立与之配套的数智化运营流程，即建立“告警接入-智能分析-自动处置-效果反馈”的新业务场景，提升事件响应速度，搭建“事前预防-事中处置-事后改进”的全周期安全运营体系。

1.事前：通过智能体的分析，识别安全告警风险和威胁情况，提供溯源分析辅助。

2.事中：智能分析助手与自动化平台、防火墙等设施联动，将应急响应时间压缩至分钟级，减少人工流程流转操作。

3.事后：通过处置结果回溯分析，自动生成改进建议，进行安全事件复盘。典型场景见图3。



图 3 网络安全数智化运营典型流程场景

同时，基于 AI+大模型的智能安全防护新思路，依托大模型海量的知识储备、上下文学习及逐步推理能力，深度落实双模型结合的威胁检测与响应机制，实现安全运营流程的自动化、智能化升级。一是应用大模型开展告警降噪与协同研判，提升网络攻击、钓鱼邮件等恶意行为的检测能力；二是基于大小双模型协同引擎架构，打造智能研判-精准处置的闭环工作流。应用大数据分析及自然语言处理技术，建立本地服务的智慧辅助决策模型，应用大模型技术建立安全事件智能响应体系，在涉及人工决策的安全运营流程中，基于大小双模型引擎协助一线值班人员进行深度分析并提供威胁处置、事件响应建议，包括忽略、跟踪、封禁等常规处置手段以及删除文件、杀死进程、重启应用等应急处置措施。

（三）关键成功要素与持续运营机制

企业构建可持续的数智化安全运营体系，需以资源集约化、能力模块化、运营闭环化为原则，通过以下核心要素与机制协同推进:

1.战略引领与组织保障

需将数智化安全运营纳入企业战略顶层设计，由管理层主导资源投入并明确责任主体(如组建虚拟安全团队或引入外部专家协同)，确保目标与业务发展同步，规避“重建设轻运营”的短期行为，形成可持续推进的组织保障机制。

2.数据治理与质量根基

以资产全景画像为起点，通过轻量级探针自动发现并整合分散的终端、云主机、安全设备等资产元数据，构建动态资产库;针对防火墙、业务系统、风险数据等多源异构日志，采用轻量化工具实现自动化采集与标准化清洗，构建“最小化可用数据池”，保障分析输入的高信噪比，为威胁检测与响应奠定可靠的数据基础，确保源头数据可信可用。基于高质量数据湖，驱动精准响应决策，形成“资产可管-数据可信-价值可释”的治理闭环。

3.技术选型与生态整合

优先选择建设一体化安全运营平台，通过开放 API 与现有 IT 系统(如办公云、业务应用)快速集成，降低定制开发与运维成本，形成经济灵活、可扩展的技术生态体系。

4.流程适配与敏捷文化

基于自动化响应能力(如剧本化处置)设计轻量化流程，利

用可视化看板实现异常透明化管理，建立周级复盘机制快速迭代策略，培育团队敏捷协作文化以应对动态威胁。

5.人才发展与安全文化

遴选现有 IT 人员接受威胁分析、应急响应等靶向培训，结合年度红蓝对抗模拟攻击检验处置能力；全员安全意识采用“强触达+轻量化”策略，将钓鱼邮件识别、密码安全等核心知识点植入日常办公流程，形成处置有专才、防御有共识的纵深文化。

6.安全与风险管理闭环

依托自动化工具定期扫描漏洞与暴露面，关联外部威胁情报生成动态风险视图，并通过工单系统跟踪处置闭环（识别-分派-修复-验证），实现风险收敛的可量化管理。

7.持续运营机制

建立数据驱动的精益改进循环：基于运营指标（MTTD/MTTR、风险处置率等）按季度评估效能，执行 PDCA（计划-执行-检查-改进）策略优化；每半年开展跨部门应急演练，确保数智化体系随业务需求弹性进化。

四、实践案例

（一）邮储银行网络安全运营数字化底座

1.网络安全运营数字化底座建设

数字化底座是网络安全运营的基础，利用大数据技术，聚合全行全网的安全数据，进行统一的标准化处理，实现整网安全数据集中纳管，并能够开放数据以及分析引擎资源，实现整网安全

能力集中协同，助力各类安全应用平滑扩展，承上启下全面激活现有分散的安全能力，为我行未来安全业务稳步发展保驾护航。

邮储银行网络安全运营数字化底座作为我行未来安全运营工作的基础支撑，实现整网安全数据统筹、分析、应用、赋能等。系统功能上，主要包括数据采集、数据预处理、数据存储、数据计算、安全引擎、服务接口、系统管理这七个主要模块，网络安全运营数字化底座架构见图 4。

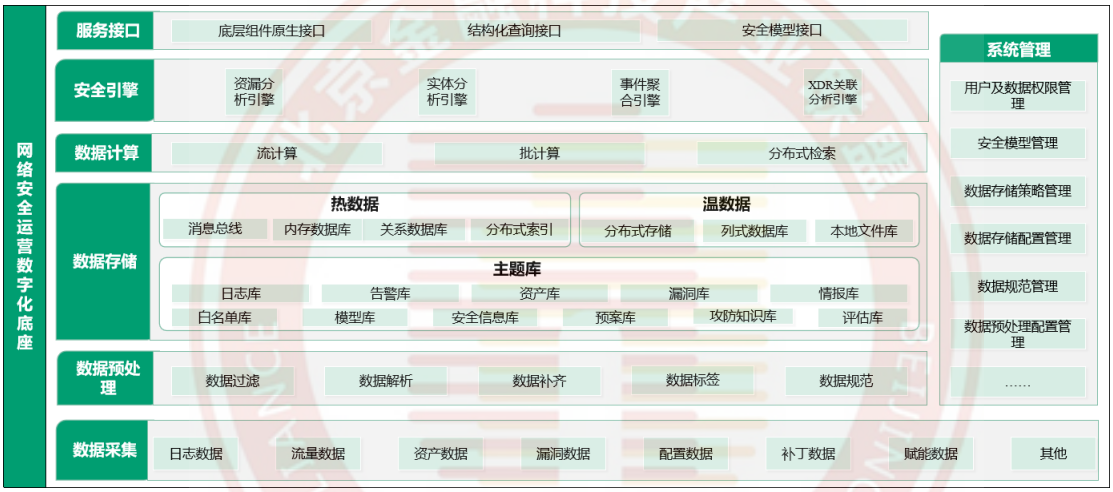


图 4 邮储银行网络安全运营数字化底座架构图

通过安全运营数字化底座建设实践，有效梳理了网络安全数据关联关系，提升我行在网络安全分析的整体水平，取得了阶段性成效，具体体现在 8 个能力。

1）数据标准化能力

通过本次实践，形成了邮储银行安全数据标准规范，其中属性标准超 1200 项，对象标准 87 项，设备标准 53 项，事件标准 85 项。根据定义的数据标准，集中采集包含安全设备、流量、终端、服务器、NAT 记录、会话、情报、资产、漏洞等 30 余类型 41

个数据源，扩大感知范围，集中管理按需索取。根据 35 类设备形成 3384 条解析规则实现自动解析，新系统配置解析，无需乙方研发，降低依赖。

2）大数据存储能力

邮储银行网络安全运营数字化底座大数据存储能力支持对海量的日志分类存储，根据数据特点和使用频率按照热、温类型分层存储，发挥不同存储类型特点，在保持查询效率的同时节约资源，同时基于主题库，增加按照日志细分类型的精细化控制存储策略，实现按类存按类查，提升查询速度的同时节约存储空间。存储能力结构见图 5。

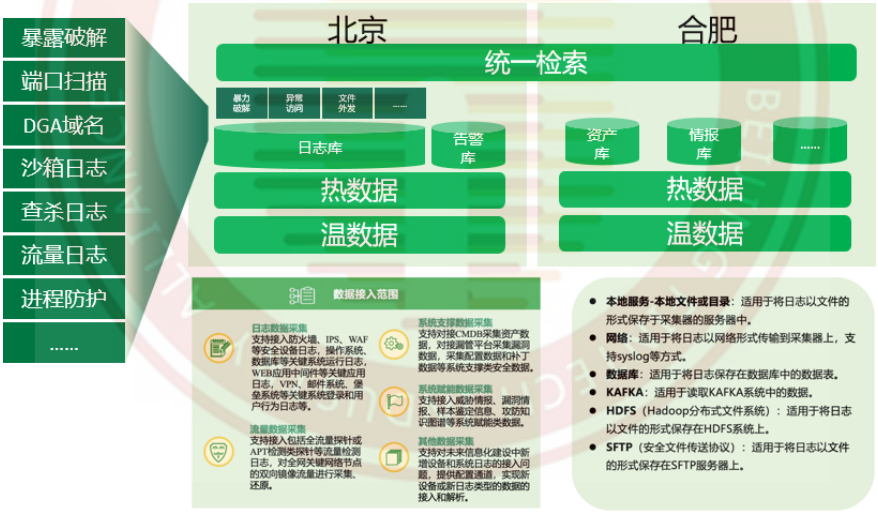


图 5 邮储银行网络安全运营数字化底座大数据存储能力结构

3）安全分析能力

网络安全运营数字化底座提供了超过 1000 条内置检测规则，并且支持自定义规则配置，15 种关联算子提升威胁检测能力。通过告警降噪、告警合并、告警策略以及事件聚合，实现超过 90%

的告警压缩，让运营人员关注少量真实攻击，提升人效比。通过事件关联多个告警时序、技战术、攻击链路图、证据、影响面、处置建议，分析研判一站完成，降低人工查询，大幅提升响应效率。通过安全分析能力的建设，数字化底座已实现日均分析 67 亿条原始日志、日均 1600 余万个原始告警。达到聚合后告警 483 万条，日均安全事件 25 条的整体效果，安全分析能力结构见图 6。



图 6 邮储银行网络安全运营数字化底座安全分析能力结构

4）风险拓线分析能力

风险拓线分析能力的建设成效可用“一页纸”“一张表”“一幅图”来表示。将资产属性与漏洞风险、攻击行为、访问关系进行关联，以风险资产为视角“一页纸”实现新漏洞或攻击特征披露后，快速发现此类问题的资产暴露面，判定风险等级。将攻击者与情报 IOC、攻击行为、攻击链深度等元素进行关联，以攻击者为视角“一张表”实现监测需重点关注的攻击者，对危害程度快速判定辅助决策响应方案。将安全实体为顶点，关联关系为线段进行关联，把风险属性与复杂关系绘制成图谱，以威胁演进为

视角“一幅图”实现根据安全线索或已知风险顺藤摸瓜，挖掘同源性等更细微的攻击痕迹，发现高隐蔽威胁或未知风险，安全拓线能力结构见图 7。

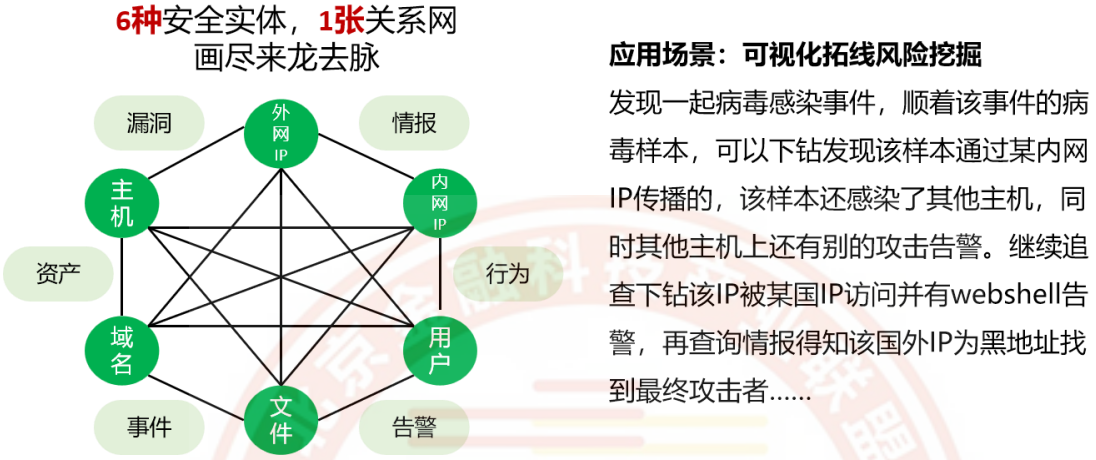


图 7 邮储银行网络安全运营数字化底座安全拓线能力结构

5）威胁狩猎监测能力

在威胁狩猎能力建设方面，数字化底座提供了 3 种数据检索模式，使用人员可以根据能力选择，并且所有类型数据统一检索入口，无需跳转多系统或页面，交叉分析提升查询效率，应用于日常运营、重保监测、可疑线索跟踪、全局协同监测等，快速应对突发状况。

6）对外服务能力

数字化底座对外提供 API 接口，并通过 API 认证鉴权方式确保接口调用安全性。平台基于核心数据采集分析能力、平台数据处理能力共开放 245 个接口，外部应用系统可基于 API 快速开发集成平台安全运营能力。此外还支持通过 syslog、kafka 将系统告警数据推送至外部应用系统，快速与外部应用共享安全原子能

力。

在对外服务过程中，数字化底座提供数据权限控制能力，通过精细化到字段级维度来划分数据权限，实现细粒度岗责分权。突破传统靠 IP 地址分权，无法满足特殊情况精确控制的弊端。不同组织的人员只能监控和运营本组织机构权限范围内的安全数据（如总行账号可以看全局，分行账号只能看自己的数据），保障安全数据最小权限访问，实现多机构、多角色安全、可信、协同运营,对外服务能力结构见图 8。

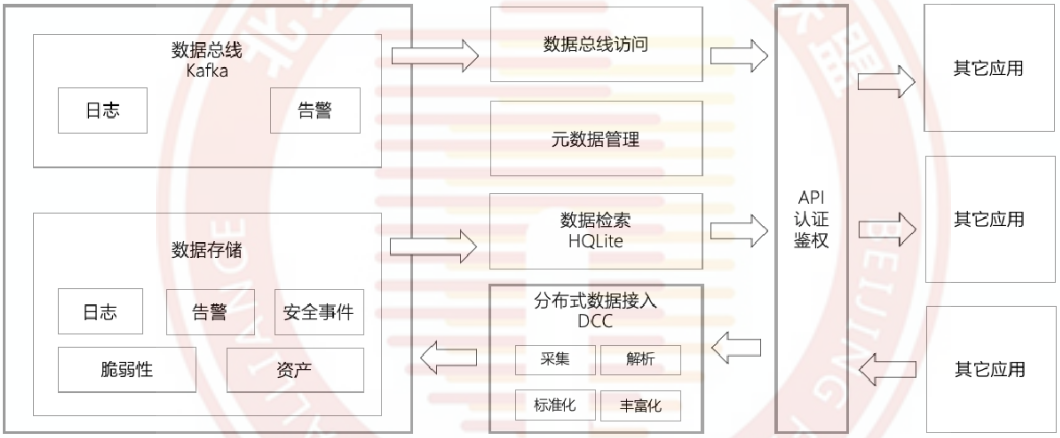


图 8 邮储银行网络安全运营数字化底座对外服务能力结构

7）系统监控能力

系统监控能力主要指自监控能力，底座提供了基于数据源、引擎组件、存储组件、业务流程等维度的全面的综合监控，可以在问题刚刚出现或潜在风险还未完全爆发时捕捉到警示信号，减少重大故障的发生频率。通过监控告警机制，运维团队可以在问题发生时第一时间接收到通知，快速采取措施，减少对业务的影响。

8）自助报表分析能力

数字化底座构建了灵活且强大的自助报表分析能力，针对日志、原始告警、合并告警、安全事件、资产、脆弱性等数据可通过拖、拉、拽快速生成分析报表且固化发布，根据不同人员关注点自行配置关注仪表盘，帮助安全分析师和决策者做出更科学的决策，同时可以更清晰地向相关人员传达安全状态和事件，提高沟通效率。

2.智能运营场景实现

基于网络安全运营数字化底座，结合大模型等人工智能技术，邮储银行结合 AI 大模型能力，探索实现智能安全运维，从而辅助安全运营人员快速研判，目前主要在以下几方面进行应用:

①利用大模型智能分析能力，对本地情报库及本地通联信息库进行匹配和关联，对 IP、hash 样本、域名等信息在本地的行为指标进行自动排查分析，判断攻击者类型，对攻击者进行深度的画像;

②通过大模型实现对威胁告警的智能研判，给出判定结论和分析过程，自动分析所有受害者资产，并提供处置建议，提升威胁告警的运营处置效率，让安全分析人员聚焦在高价值的安全事件处置上;

③利用大模型意图理解转化能力，在网络安全大数据平台中使用自然语言描述需要检索的数据内容，实现自然语言转译为平台能够识别的类 SQL 语言的“智能问数”。

同时，结合领域知识+RAG+运维工具，打造“一站式”运维问题智能解决助手，目前安全场景已在以下两方面提供服务：①整合各类运维知识、制度文件实现运维问题快速检索问答；②结合大模型分析能力和海量运维数据信息，通过自然语言问答，实现数据查询分析及图表生成。

（二）北银金科聚焦高危场景践行“AI+SOAR”

在网络安全运营数智化转型中，北银金科通过“AI+SOAR”平台实现日均 3000 条低风险告警自动化处置，将人工处理量压缩 70%，其关键在于聚焦高危场景构建攻击链模型。实施中曾遭遇数据孤岛问题，后通过建立跨部门白名单机制，优先整合支付系统与终端日志破局。

在企业内部安全运营管理中，运营流程的数智化重构成为企业安全运营体系升级的核心引擎，旨在通过数据驱动与智能技术实现安全运营的自动化、智能化、协同化与持续优化。在网络安全数智化转型中的运营流程重构方面，北银金科并不是推倒重来，而是基于现有管理流程和技术手段作为基础，用数据+智能技术对漏洞管理、风险评估、事件响应等多个流程进行“精装”，目标是看得更清、反应更快、处置更准。

1.核心目标和落地原则

运营流程的数智化重构核心目标体现在最务实的点上是先帮运营团队减负，再帮运营团队提质增效，北银金科利用自动化编排技术、人工智能技术、大数据分析技术把一线人员从重复筛

选告警、填写工单、大量手动操作的常规工作中解放出来，让更多的安全分析脑力集中在深度分析和价值挖掘，把日常安全管理工作和威胁告警处置的 MTTD/MTTR 缩到最短，通过核心流程的自动化建设，如自动化封禁 IP、一键处置威胁告警等让威胁初期得到有效控制，后续在流程优化中再精准打击，降低误报率，提高高危威胁检出率，最后再让风险整体可视化，打破流程孤岛，实现跨团队、跨系统的高效协同处置，借助安全运营管理平台建立“监测->分析->响应->反馈->优化”的完整数据闭环。实施落地坚持“小步快跑、数据先行、可信 AI、流程前置”五项原则：以 MVP 快速验证 ROI，复用 SOC/漏扫等存量系统并通过标准 API 打通，先完成日志规范与数据质量治理，再部署自动化编排剧本并保留人工确认闸口，最终在事件响应 SOP 固化后方可转化为可审计、可回滚的 SOAR 剧本。

2.核心流程的重构实践

面对传统响应模式下告警处置依赖人工电话协调、手动执行封禁与取证导致的效率瓶颈，以及业务影响难评估、经验知识碎片化等痛点，北银金科安全运营团队通过一体化安全运营平台和 SOAR 驱动的智能协同闭环机制实现转型。

北银金科基于高频威胁场景（如主机失陷、暴力破解、恶意流量攻击）构建标准化响应剧本，依托 SOAR 平台打通防火墙、堡垒机、CMDB、工单管理等系统接口，实现从告警触发到初步遏制的全链路自动化：系统自动提取威胁主体信息并联动安全设备

执行网络隔离或端口封禁以阻断攻击扩散，同步内存快照、网络连接等关键证据链，同时一键补充资产信息（关联 CMDB 业务归属）及处置记录的工单推送责任人，将 MTTR 压缩 30%以上，尤其保障非工作时段核心业务的快速回正。

通过构建数智化运营流程，实现一键协同，打通安全人员、业务负责人协作通道，实现处置过程全链路可视化追踪与指令同步；事件闭环后自动输出结构化报告，整合操作时间轴、明确影响范围。

3.关键支撑与整体应对

在推进运营流程数智化重构进程中，北银金科正着力构建三大核心支撑体系：一是打通数据动脉，联合运维部门推动网络设备及各个工具平台数据整合，夯实数智化根基；二是强化平台协同，通过 API 深度集成 SOC、SOAR、防火墙等既有工具能力，破除工具孤岛；三是推动团队转型，小组成员聚焦数据分析、剧本开发、流程设计等专项技能提升，通过内训外联加速能力进化。

北银金科的实践展现了中小企业数智化转型的务实路径：面对资源限制，精准锚定三大高危场景构建防御体系，通过自动化处置释放运维压力。其价值不仅在于技术落地，更在于破解困局的智慧——当数据孤岛阻碍进展时，以业务共识优先打通关键节点，建立跨部门白名单机制实现快速破冰。值得注意的是，这种轻量化模式在提升效率的同时，仍需警惕自动化盲区对深度威胁的遮蔽风险。这一案例为区域性金融机构提供了重要启示：在有

限条件下，通过场景聚焦、渐进整合与风险平衡，同样能构建有效的安全运营框架，其核心在于把握关键矛盾并采取折中可行的解决方案。

（三）兴业银行基于大模型智能体重构安全运营

1.业务场景梳理

兴业银行针对网络安全运营中“告警量大、分析复杂、误报率高”等突出痛点，首先对现有业务场景进行了系统性梳理，明确了数智化转型的关键切入点。

1）告警聚合处理。通过对海量告警进行去重、归类和聚合，构建事件维度的集中分析视角，有效压缩待研判信息量，减轻一线运营负担。

2）人工研判流程建模。梳理运营人员处置告警的关键步骤，包括信息收集、情报关联、上下文分析、误报排查、生成处置建议等，构建可复用的研判逻辑链条。

3）元数据清洗机制。针对原始日志格式不一、字段缺失、命名不规范等问题，设计自动清洗模块，标准化资产、情报、告警等多源异构数据，确保研判数据的完整性与准确性。

2.大模型能力构建

兴业银行基于 LangGraph 多智能体框架，构建了“安全告警分析助手+安全运营智能体”双组件协同架构，实现从数据获取到处置决策的闭环自动化，能力技术架构见图 9。

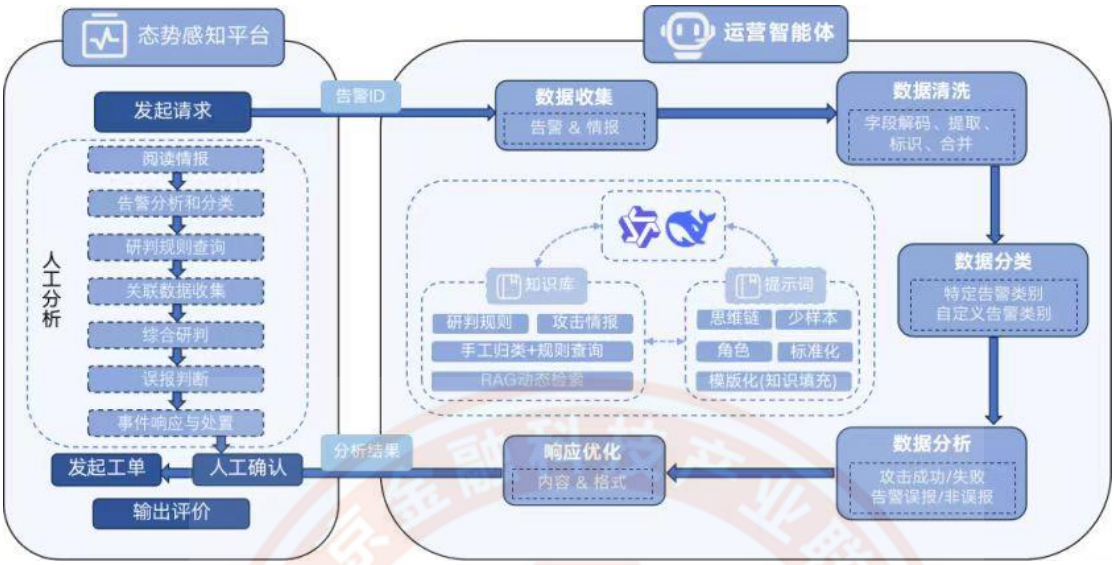


图 9 兴业银行大模型能力技术架构图

（1）安全运营智能体：聚焦模拟人工研判过程，主动获取原始日志与关联信息，完成数据清洗、结构化处理，结合知识库与提示词对告警进行分类、上下文关联与误报判断，模拟运营专家的思考路径生成分析结论。

（2）安全告警分析助手：作为运营人员的操作入口，支持点击式调用智能体对当前告警进行分析，分析结果以结构化形式呈现，并根据研判结果自动跳转至相关处置系统（如封禁、发单、复核等），提升操作连贯性和效率。

3. 业务场景融合

兴业银行在引入大模型能力前，安全运营中的告警分析和误报复核流程高度依赖人工操作。运营人员需要手动查看告警详情，逐一查找对应的情报、资产等信息，基于个人经验进行判断，再完成处置或复核操作。整个过程操作链条长、信息分散、效率较

低，且结果受个体差异影响较大。

引入大模型后，系统以“安全告警分析助手 + 安全运营智能体”为核心，全面重构运营流程。运营人员在面对告警时，仅需通过“安全告警分析助手”一键发起分析请求，智能体便会主动调用接口获取告警原始日志、关联资产信息、漏洞情报以及历史处置结果，完成清洗处理和综合分析，并将分析结果结构化输出。在告警分析场景中，助手会直接展示智能体生成的研判结论和处置建议，运营人员可在此基础上快速决策，并一键发起处置，无需跨系统查找信息，大幅缩短处理时长。在误报复核场景中，分析助手将同步呈现三类关键信息：当前告警的原始信息、运营人员的人工处置描述，以及大模型智能体的分析结论。复核人员可在一个界面内对比人工研判与模型研判差异，进行快速复核与再判断，并立即发起误报确认或修正操作，场景流程方案见图 10。

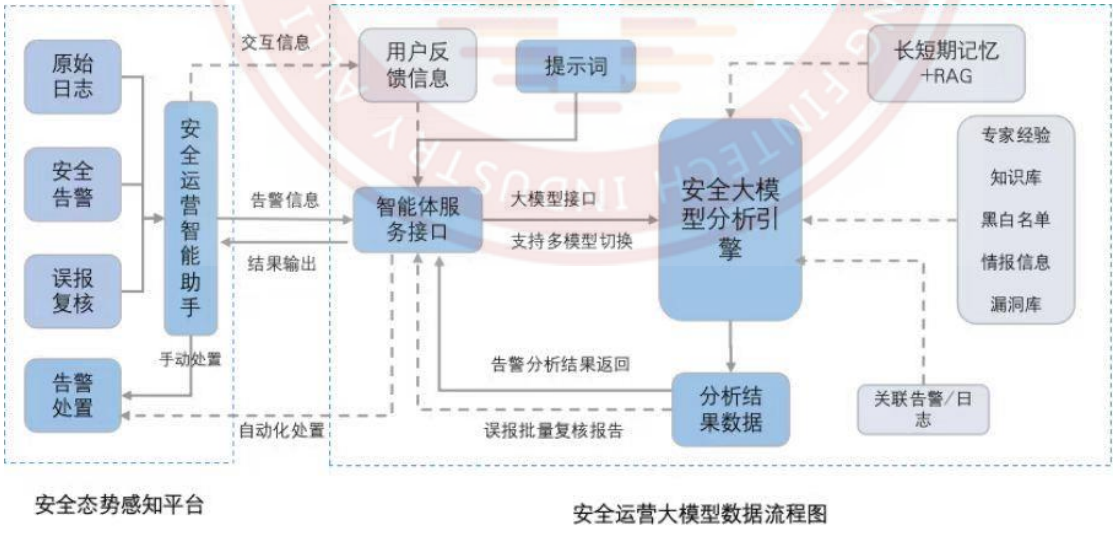


图 10 兴业银行场景流程方案

这一变革将原本“人找数据、人做判断”的流程转变为“系统

找数据、系统输出建议、人确认决策”，显著提升了处置效率和分析一致性，推动安全运营从人工为主向智能驱动转型。

4.智能分析能力提升优化机制

系统在运行过程中，持续比对大模型分析结果与运营人员最终处置结果的差异，通过以下方式进行闭环优化:

1）分析差异背后的提示词覆盖盲区、知识不足等问题;

2）动态调整和升级提示词策略，补强上下文引导精度;

3）梳理流程链条中断点，优化交互路径和响应逻辑;

4）基于人工复核结果，反哺模型推理逻辑，提升判断准确率和业务适配度。

该机制实现了“模型分析-人工复核-反馈优化”的迭代闭环，推动大模型能力持续进化，形成“越用越准”的智能运营体系，显著提升了告警分析质量、效率和用户体验。

（四）浙商银行构建“一基础五平台”数智化防护体系，实现平战一体化安全运营

浙商银行围绕网络安全可防护、可感知、可运营、可验证的目标，提炼防护、分析、调度、决策、验证等五大基础能力，梳理形成安全能力图谱，并持续迭代升级“一基础五平台”安全架构，实现端到端的网络、系统、应用、数据一体化安全调度，打造全链路、全资产、全感知、全流程和快预警、快响应、快处置的数智化网络安全防护技术体系，体系架构详见图 11。

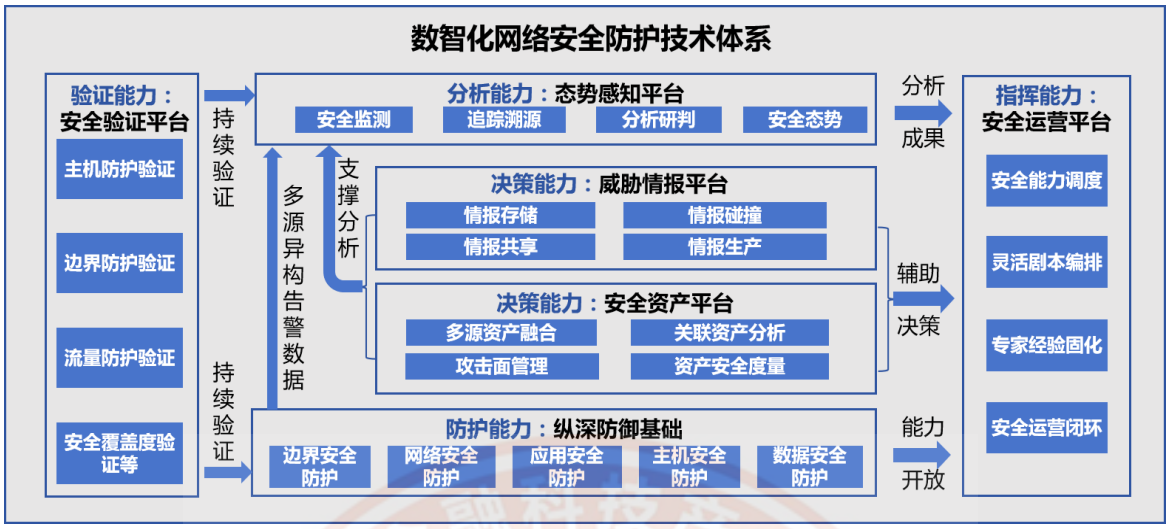


图 11 浙商银行数智化网络安全防护技术体系框架

该体系中**纵深防御基础**提供边界、网络、应用、主机、数据等层面的安全防护能力，**安全资产平台**和**威胁情报平台**输出资产与情报信息赋能分析与决策，**态势感知平台**汇聚多源数据进行关联分析并产出降噪后的告警，**安全运营平台**统一调度安全原子能力完成安全事件闭环处置，最后**安全验证平台**常态化检验体系有效性。

依托数智化网络安全防护技术体系，该行切实落地以“持续监测、精准识别、智能响应、快速处置、自动闭环”为目标的安全运营机制，形成“7×24 小时持续、主动、全面”的网络安全有效防护。

1. 运营场景数智化

安全运营平台上接态势感知平台海量降噪告警，下联 20 余项行内系统和安全设备，通过安全编排自动化与响应技术，实现告警分析、威胁响应等安全运营任务高效、准确地自动化执行，

将全量安全运营工作迁移至安全运营平台开展，极大提升安全运营效率。

2. 平战切换一体化

为提升实战对抗能力，围绕常态化、高强度、无间断的保护目标，针对平时运营“精且准”、战时处置“快又狠”的差异化需求，该行从纵深防御能力、威胁研判策略、威胁响应策略、资源配置策略四个维度建立平战策略切换机制，详见图 12。平时稳健保障，减少安全防护工作对业务的影响；战时全面戒备，通过平战策略快速切换，扩展纵深防护范围、提升威胁响应力度，实现平战差异化场景下的一体化运营。

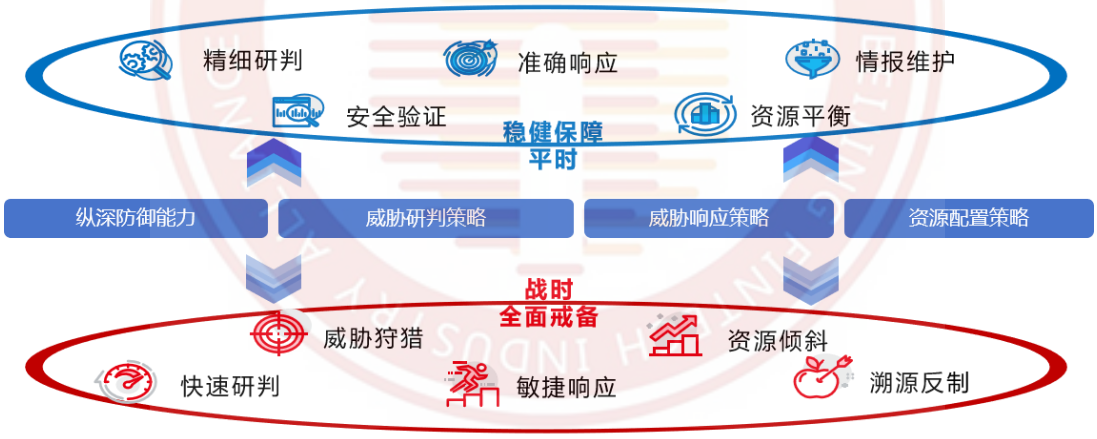


图 12 平战策略切换机制

3. 安全资产多源化

安全资产平台对 CMDB、主机安全、防病毒等资产源数据每日进行采集分析，形成完善的安全资产及漏洞管理台账；同时对资产的内外网映射关系进行配置，展示清晰的互联网应用和内访

外链路，为资产清点、风险发现、攻击溯源提供可视化资产数据支撑。

4.安全态势可视化

该行以等级保护、网络安全能力成熟度评价模型为指导，沉淀安全建设与运营经验，形成安全态势运营指标体系，基于态势感知平台提取汇聚指标数据，构建安全运营数字化驾驶舱，面向不同场景细化可视化大屏设计，涵盖安全运营指标监控、安全防护覆盖情况监控、网络安全事件处置监测、网络区域告警监测、重保态势等场景。

五、未来展望

展望未来，银行业网络安全运营将全面迈向以“数智融合、主动免疫、价值共生”为核心理念的智慧运营新阶段，实现从战略、组织到能力的全方位重塑。

（一）AI 重塑安全运营内核

未来，安全运营的中心将是具备自学习、自进化能力的 AI 大脑，依托于汇聚全行海量数据的安全数据中台，通过大语言模型和生成式 AI 技术实现智能研判与自动化响应，能够前瞻性地主动狩猎隐藏威胁，并将安全风险动态量化为可与业务影响直接关联的指标，使安全从成本中心转变为清晰可见的价值守护者。

（二）构建开放共生安全生态

未来的银行安全将超越自身边界，积极融入更广阔的安全生态，通过区块链、隐私计算等技术在保护隐私的前提下实现行业

威胁情报的安全共享与协同防御，并将第三方供应商的安全状态纳入统一监控，实现从代码到云端的全链路安全管理，系统性地提升整体安全水位。

（三）重塑安全团队组织形态

数智化运营将推动安全团队组织形态的进化，安全专家将从繁琐的告警处理中解放，转型为 AI 模型的训练师和复杂事件的决策者，同时借助自然语言交互界面，业务人员也能直观获取安全洞察，从而实现安全能力向全员的赋能，形成高效的人机协同新范式。

未来的银行业网络安全数智化运营将演变为一个高度自主、内外协同、价值驱动的“智慧生命体”，通过将安全能力无缝嵌入每个业务流程，最终为银行业的数字化转型构筑起一道坚固而灵动的“数智免疫防线”。